Loveland/DellaBetta
✓ FILED ___ ENTERED
___ LOGGED _____ RECEIVED
9:22 am, Jun 02 2021
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____Deputy

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF:	
2700 MURA STRET, BALTIMORE, MARYLAND ("TARGET RESIDENCE 1")	1:21-mj-1165 TMD
739 N. KENWOOD AVENUE, BALTIMORE, MARYLAND ("TARGET RESIDENCE 2")	**Filed Under Seal** 1:21-mj-1166 TMD
5116 PEMBRIDGE AVENUE, BALTIMORE, MARYLAND ("TARGET RESIDENCE 3")	**Case No.** 1:21-mj-1167 TMD
THE PERSON OF YUSEF GALES-BEY	1:21-mj-1168 TMD
THE PERSON OF DEQUAN ELLIS	1:21-mj-1169 TMD
THE PERSON OF DARRELLE RICH	1:21-mj-1170 TMD

AFFIDAVIT IN SUPPORT OF
APPLICATIONS FOR SEARCH WARRANTS

I, Special Agent Summer Baugh, Federal Bureau of Investigation ("FBI") being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I submit this affidavit in support of applications pursuant to Federal Rule of Criminal Procedure 41 for the following search warrants:

A. TARGET RESIDENCES 1-3

2. I request authorization to search the following locations :

i. The premises located at 2700 Mura Street, Baltimore, Maryland 21213 ("**TARGET RESIDENCE 1"**), described in **Attachment A-1**;

ii. The premises located at 739 N Kenwood Avenue, Baltimore, Maryland 21205 (**"TARGET RESIDENCE 2"**), described in **Attachment A-2**;

iii. The premises located at 5116 Pembridge Avenue, Baltimore, Maryland 21215 (**"TARGET RESIDENCE 3"**), described in **Attachment A-3**; and

TARGET RESIDENCES 1-3 are also referred to collectively as the "**TARGET RESIDENCES**."

3. As described further in this affidavit, I submit probable cause exists to believe that the **TARGET RESIDENCES** contain evidence, fruits, and instrumentalities of the following offenses: Interstate Threats (18 U.S.C. § 875), Obstruction of Justice (18 U.S.C. § 1503); and Witness Tampering (18 U.S.C. §§ 1512, 1513). Collectively, these offenses are referred herein as the **"SUBJECT OFFENSES**." The property to be searched for and seized from the **TARGET RESIDENCES** is described in **Attachment B**.

B. THE PERSONS OF YUSEF GALES-BEY, DEQUAN ELLIS, AND DARRELLE RICH

4. As described in this affidavit, I submit probable cause exists to believe that a search of the persons of the following individuals (collectively, the "**TARGET SUBJECTS**") may reveal evidence, fruits, and instrumentalities of the **SUBJECT OFFENSES**: Yusef **GALES-BEY** (described in **Attachment A-4**), Dequan **ELLIS** (described in **Attachment A-5**), and Darrelle **RICH** (described in **Attachment A-6**). The property to be seized from the **TARGET SUBJECTS** is also described in **Attachment B**. As discussed further in this affidavit, investigators believe the

TARGET SUBJECTS each presently reside at a given **TARGET RESIDENCE** in the District of Maryland.

5. Because this affidavit is being submitted for the limited purpose of establishing probable cause for search warrants, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of the aforementioned federal statutes are located within the **TARGET RESIDENCES** and/or on the persons of the **TARGET SUBJECTS**. I have not, however, excluded any information known to me that I believe would defeat a determination of probable cause. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, police officers, witnesses, telephone records, sources, and reports.

AFFIANT BACKGROUND

6. I am a Special Agent with the FBI and have been since 2015. As such, I am an officer of the United States who is empowered by law to conduct investigations of and to make arrests for violations of federal law.

7. During my employment as an FBI Agent, I have been assigned to investigate violations of federal law such as bank and armored carrier robberies, armed commercial robberies, the apprehension of federal fugitives, extortion, and kidnapping with the FBI Violent Crimes Task Force in Baltimore, Maryland. I have participated in the execution of search warrants in various types of investigations involving searches and seizures of mobile phones, computers, computer equipment, electronically stored information, email accounts, and social media accounts. I have also received training and gained experience in the areas of computer crime investigations, cellular analysis, and the location and tracking of cellular telephones.

8. Based on my knowledge, training, and experience, I am aware that fruits and instrumentalities of criminal activity are often concealed in digital form. Furthermore, digital technology is often used to store evidence of criminal activity. Individuals who participate in collective criminal activity, including extortion, frequently utilize cellular telephones to commit their crimes and frequently communicate with one another by cellular telephone and by social media and use of the Internet before and after those crimes. I know that individuals will use cellular phones and communication applications to identify victims they plan to extort, to communicate with co-conspirators to plan the extortion, to communicate with victims during the extortion offenses, and to communicate with co-conspirators on how to split the proceeds of the extortion or dispose of evidence that the extortion was committed. This is especially true when the same individuals commit multiple extortionate acts against multiple victims. I also know that individuals engaged in online criminal activities often will use multiple usernames and email addresses in an effort to hide their true identities or locations, but may use the same physical device to access those multiple accounts. I also know that the use of cellular telephones includes social media applications installed and accessed from the phones, including Instagram and Google accounts.

9. Based on my training, knowledge, and experience, I know that the location of a cellular phone at a particular time (based on cell-site records and location information) may constitute evidence of a crime. Such location information allows investigators to determine, for example, whether a particular telephone was in the vicinity of a known address of an offender, and whether that particular telephone was utilized for significant periods of time by the same user.

10. Based on my training and experience, I know that instant messages, emails, voicemails, photos, and videos—all of which may be saved on a user's physical device—are often

created and used in furtherance of collective criminal activities, including extortion. I also know individuals may take photographic images of communications or social media posts taken in connection with the crimes committed, to share that information with others, or to store it on electronic devices. More specifically, I know that members of collective criminal activity use cellular telephones to further their objectives by, among other things, communicating with other co-conspirators by talking and by text messages, including iMessages; and taking photographs and recording videos of co-conspirators and contraband. Furthermore, based on my training and experience, I know that such communications, photographs, and other information may be found on an individual's cellular device, as well as Cloud-based accounts.

11. I know, based on my training, knowledge, and experience that that web-based communication accounts, such as those provided by Facebook, Instagram, Apple, and Google are increasingly common ways for persons to communicate. Further, I am aware that Facebook and Instagram users often use the messaging and posting functions to provide alternate contact information, such as additional Facebook and Instagram accounts, e-mail accounts, phone numbers, and/or other social networking contact information in order to continue and facilitate their communications privately. Further, I am aware that Facebook, Instagram, Apple, and Google allow users to communicate privately. Facebook and Instagram accounts often contain phone numbers, email addresses, messages and/or emails, photos, and other registration information. Similarly, Apple, Google, and Cash App accounts may also contain phone numbers, alternate email addresses, messages and/or emails, financial information, photos, other registration information as well as location information. Furthermore, based on my training, knowledge, and experience, it is common for suspects who commit extortion to use social media and email

accounts to communicate about their crimes. I know that information from these accounts is often contained within a cell phone.

12. I know, based on my training and experience, that suspects who commit extortion may maintain books, records, receipts, notes, ledgers, money orders, and other papers relating to the payment of extortion demands; the proceeds derived from those transactions; and the identities of and contact information for their victims or co-conspirators; and that they may maintain these items in secure locations where they have ready access to them, including in the residences and vehicles they use.

13. Based on my training and experience, I know that it is common for offenders to secrete records of extortion demands and payments, amounts of currency, and financial instruments in secure locations within residences, including in combination or key-lock safes or strong boxes, suitcases, locked cabinets, and other types of locked or closed containers, and hidden compartments, not for only ready access but also to conceal them from co-conspirators and law enforcement.

14. I know, based on my training and experience, that suspects who commit extortion amass proceeds from their crimes and attempt to legitimize those proceeds and that, to accomplish this goal, utilize domestic banks and their attendant services, securities, cashier's checks, electronic money transfer services, or prepaid credit or debit cards, and that offenders commonly keep records of these transactions in secure locations like residences.

15. Based on my training and experience, I know that in residences or other secure locations, offenders typically maintain identification and indicia of occupancy, residency, and/or ownership of the premises. I also know that offenders often place cellphones, vehicles, residences, and other assets in names other than their own to avoid law enforcement surveillance or forfeiture

and that, even though these items are in another entity or person's name, the offenders actually own and continue to use these cellphones, vehicles, residences, and other assets.

16. In my training and experience, I have learned that providers of cellular telephone service have technical capabilities that allow them to collect and generate information about the locations of the cellular telephones to which they provide service, including cell-site data, also known as "tower/face information" or cell tower/sector records. Cell-site data identifies the "cell towers" (*i.e.*, antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (*i.e.*, faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate location of the cellular telephone but is typically less precise than other types of location information, such as E-911 Phase II data or Global Positioning Device ("GPS") data.

17. Based on my training and experience, I know that wireless providers typically collect and retain cell-site data pertaining to cellular phones to which they provide service in their normal course of business in order to use this information for various business-related purposes. Wireless providers also typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless telephone service.

18. I also know that wireless providers typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications

sent or received by a particular phone and other transactional records, in their normal course of business. In my training and experience, this information may constitute evidence of the crimes under investigation because the information can be used to identify the target device, its users(s), or the location of the cellular device at a given time, which may assist in the identification of co-conspirators and/or victims.

19. Based on the facts set forth in the affidavit, there is probable cause to believe that the **TARGET SUBJECTS** are involved in the above-described federal offenses. There is also probable cause to believe that the **TARGET RESIDENCES** may contain evidence, fruits, and/or instrumentalities of the **SUBJECT OFFENSES.**

INVESTIGATIVE FACTS

20. The Baltimore Police Department (BPD) and the Federal Bureau of Investigation (FBI) are investigating a series of Instagram posts that contained extortionate threats targeting alleged law enforcement cooperators and witnesses and labeled said cooperators and witnesses as snitches, rats, or other derogatory terms. Some of the online threats requested payment for either removing witness information from dedicated Instagram pages, or for never posting information at all. The witnesses/cooperators whose information was posted online reside in multiple counties in the state of Maryland and some have provided assistance to law enforcement in state and federal investigations during the past five years.

Initiation of Investigation

21. On August 25, 2020, BPD Homicide Detectives were contacted by a family member of a witness in an active criminal case. The family member provided screenshots from Instagram page “ratsofbmoe” where the name and photograph of the witness was posted, along with documentation claiming the witness was cooperating with police. A review of the

"ratsofbmoe" Instagram page revealed photographs of approximately 33 different individuals the poster collectively labeled as "rats." Posts were accompanied by some form of "paperwork", which included law enforcement statements of probable cause, state court transcripts, and signed photo arrays that gave details regarding how each witness assisted police. I know from my training and experience that "rat" is a derogatory term used to describe an individual who provides information to law enforcement about another person's criminal activity or who otherwise cooperates with law enforcement.

22. BPD initiated a witness intimidation investigation and contacted the FBI. A cursory review of Instagram revealed multiple variations of the "ratsofbmoe" page, several of which contained threats and extortionate posts directed at identified witnesses. The pages appeared to be related based on similarities in their names, profile photos, content, and explicit or circular references to each other. Based on this information, a federal investigation was opened.

Identification of Additional Instagram Accounts

23. Shortly after the initial report to BPD, the "ratsofbmoe" Instagram account was no longer active. Detectives identified "ratsofbmoe2", which had over 4,500 followers and a caption that stated, "Back up !! stay posted <smiling emoji and rat emoji>." There were initially no public posts on the page because the account was labeled as private.

24. On August 31, 2020, Instagram page "ratsofbmoe3" was located by BPD. Posted on that account were 34 photographs of possible witnesses to criminal cases with comments about their testimony or statements made to police. The caption written by the author of the page stated, "itsMeSnitches… If you Ratted In Any Way Shape Or Form I'm On Ya Ass Idgaf If The Target Dead Or Alive…" I know that "Idgaf" is an abbreviation for "I don't give a fuck." I also know that "snitch" is a derogatory term with a meaning similar to that of "rat". This account used as a

profile photo a cartoon depiction of a rapper who goes by the performance name Tekashi6ix9ine holding a piece of cheese. In well publicized court documents and media reports, Daniel Hernandez, also known as Tekashi6ix9ine, received a reduced sentence on federal conspiracy to commit murder and armed robbery charges in exchange for testifying against Bloods gang members in 2019.

25. On September 1, 2020, Instagram page "ratsofbmoe1" was located, and a review of the page revealed photographs of 36 different individuals posted, which included information about the cases that they allegedly testified in or investigative documents showing how they assisted law enforcement or served as witnesses. Many of the individuals and photos posted were identical across "ratsofbmoe", "ratsofbmoe1", "ratsofbmoe2", and "ratsofbmoe3", suggesting they were controlled by the same person, or by a group of individuals working together to share information.

Links Between Accounts

26. By late September 2020, over ten Instagram accounts were identified that contained variations of the "ratsofbmoe" name. In addition to similar display names, profile photos, and content posted on the accounts, multiple references between pages were also located. For example, a post observed on September 21, 2020 by "ratsofbmoe3" stated, "Follow @returnoftherats_ofbmoe I'm One Strike Away From Being Deleted." A similar caption was observed on "darealratsofbmore", which stated, "Follow this page cuzz the other one gone get blocked." Additionally, several "ratsofbmore" pages "follow" other "ratsofbmore" pages. The number of followers for each page ranged from below 100 to nearly 7,500 on "darealratsofbmore." Several of the pages were marked "private", meaning content is not visible unless an Instagram user requests to "follow" the page and is accepted by the page owner as a "follower."

27. On November 24, 2020, a United States Magistrate Judge, the Honorable Thomas M. DiGirolamo authorized search warrants for ten Instagram accounts, including those detailed above, in addition to other social media accounts. A review of information provided by Instagram revealed multiple messages sent by "ratsofbmoe3" to other Instagram users stating the account holder would not accept payment for removing individuals posted on the page. However, further review of the account's private messages revealed the following exchange with "ratsofbmoe1", suggesting the accounts were controlled by two different individuals who may be working together:

> **ratsofbmoe3**: If ya page get deleted let me know I'm backing up all the info you got on this page broski
> **ratsofbmoe1**: Yoo u stealin my shit
> **ratsofbmoe3**: Nooo bruh it's not like that after ya last 2 got deleted I made it shit if you want it I'll give you the password and all
> **ratsofbmoe1**: Naw bro I don't want nobody else doin it in case something fake come up
> …
> **ratsofbmoe3**: All I'm doing is repost nothing more
> **ratsofbmoe1:** Bet what's the password
> **ratsofbmoe1:** I'm bout log in
> **ratsofbmoe3:** I got you let me change my email and take my phone number off it

Extortionate Posts, Threats, and Information Posted about Federal Cooperator

28. A review of "ratsofbmoe1" on September 4, 2020, revealed the following posts: "I'm doin deal before 12 pm 75$ I take ya paper work down for a day <*laughing emoji, laughing emoji, male facepalm emoji*> stack I delete it for good stomp y'all fkn feet." I know from my experience that a "stack" often refers to a sum of $1,000. In another post, the user stated, "Why tay ain't say he want his lawyer why he talk <*five rat emojis, four pencil emojis*> I wouldn't have him up there if he ain't rat I don't slander I extort I mean expose." A third post read, "I'm lookin at my cash app and I don't here stomping now if u ratted and I ain't posted u yet do the right thing

reach out and cash app cuzz once I post u the whole city gone see it."

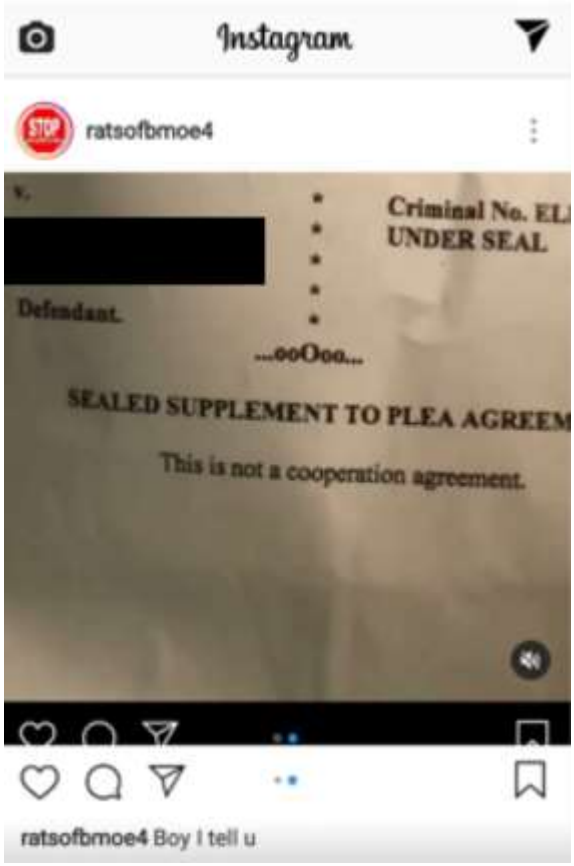
29. Several additional pages and posts were identified that repeated extortionate threats demanding payment for removal of an individual's information from public Instagram pages, or advance payment to prevent information from being posted in the first place. For example, on September 17, 2020, "ratsofbmore1" posted the following:

> "Stomp yalll fkn feet 100$ a day 1000$ get ya bitch ass down for good u know u told on a nigga why u sittin there contemplating hit da cash app cuzz once u posted all the bad bitches in da city got ya paper works <*three rat emojis*>."

30. On September 23, 2020, "ratsofbmore_" captioned:

"Posting all the rats in Baltimore City <two laughing emojis, rat emoji> cashapp me to come down." At the time, the page did not contain any posts and had 90 followers.

31. On September 17, 2020, "ratsofbmoe4" posted a Sealed Supplement to a federal plea agreement with a Defendant's name visible. The text of the document stated, "This is not a cooperation agreement." Instagram user "ratsofbmoe4" commented, "Boy I tell u."



Instagram posts on "ratsofbmoe4" observed on 09/17/2020[1]

32. On September 30, 2020, "ratsofbmoe4" posted, "Kill all rats <*rat emoji*> flat out <*head explosion emoji, bb gun emoji*>." Also posted was a victim's photograph with a bb gun emoji pointed at the victim's head. On the other side of the victim's head was an emoji of a head exploding. Underneath read text, "Famous go hard rat".[2]

33. In addition to extortionate threats posted publicly on Instagram, a review of private messages obtained pursuant to search warrants identified communications where federal paperwork was solicited and/or sent via Instagram, and was later posted publicly, including the

[1] While the above was captured by viewing the publicly visible post, a review of content posted by this account after a federal search warrant was obtained failed to locate this post, indicating that it may have been deleted prior to the account being preserved.
[2] This victim has not yet been identified.

identification of federal cooperating witnesses. For example, on August 24, 2020, Instagram account "butta1983" sent "ratsofbmoe1" a picture of a federal plea agreement. In addition to photos of federal paperwork, pictures of the defendant were also sent by "butta1983" to "ratsofbmoe1." The information was later posted publicly by "ratsofbmoe1", including additional pages of the plea agreement with text added suggesting that based on the sentence the individual received, he or she must have cooperated with authorities. "Ratsofbmoe1" wrote, "(under Federal Guidelines when u sign off under the "ACCA" it's a Mandatory 15 Years. google it. only way u can get under 15 years is if u get a 5K.1 departure for snitching." On another post was the text, "go to www.pacer.gov Case Number [***##-####] for original documents.. this is PUBLIC RECORD!!! the people have the right to know.. HE CAME HOME LAST YEAR (2019)…" On August 25, 2020, Instagram account "2stroketommy" contacted Instagram account "ratsofbmoe1" and sent a picture of a federal plea agreement with the defendant's name visible. Investigation revealed that this person had, in fact, served as a cooperating witness.

Identification of Victims

34. Investigators believe the Instagram accounts were created to target individuals who served as witnesses or cooperated with law enforcement and label them as "rats" and "snitches" who are deserving of repercussions, to include physical injury or death. Being labeled a "rat" on a public social media page also appears to be an attempt to intimidate individuals and prevent them from providing information to the police or from testifying in court when required to do so. Thus, the posts undermine the legal system and the ability for the courts and law enforcement to perform their lawful duties in the administration of justice. Further, some of the comments on these Instagram pages contained death threats against "rats" in general, and also against specific individuals posted as "rats." Additionally, the accounts made multiple posts concerning soliciting

payment in order to remove content. The word "extort" was used explicitly. It therefore seems that the posts and threats (explicit and implicit) of repercussions were made with the intent to extort money from victims and witnesses.

35. To date, BPD has identified approximately 36 individuals posted on the above Instagram pages. Investigators have made contact with several of them to determine if they have received any direct threats or have concerns for their safety based on the information posted about them online. One victim was interviewed and stated, in substance, that he was sent a text message containing the post of his personal information on one of the above-mentioned Instagram pages. Shortly after that, the victim was confronted on the street by an associate of the person who texted him. The associate pulled a gun on the victim and called him a "rat." This example illustrates the concern law enforcement has for the safety of witnesses and victims based on the posting of the information made by these accounts. It also illustrates why people may be dissuaded from appearing for court or cooperating with law enforcement, thus the posts on these accounts serve to undermine and obstruct the administration of justice.

36. At least one of the individuals identified on "ratsofbmoe3" is deceased. A comment posted by "ratsofbmoe3" next to paperwork describing cooperation with law enforcement stated, "Was this page active before he died NO was his paperwork sent to me YES Dead or Alive I Will Tell The Story."

37. Investigation to date has revealed at least two verified federal confidential sources or cooperators were posted by at least one of the **TARGET SUBJECTS**. A victim who was identified as a confidential source in a separate federal narcotics investigation and hereinafter "CS-

1"[3] , engaged in a direct message conversation on Instagram with the user of "ratsofbmore1" at the request of CS-1's handling agent. During the private conversation, the user of "ratsofbmore1" told CS-1, "75$ I take it down right now." At this time, no payment has been made by CS-1 in exchange for removing CS-1's information from Instagram, as "ratsofbmore1" did not provide a money transfer platform or account to send payment to, after CS-1 inquired about how to make payment.

Identification of the TARGET SUBJECTS and TARGET RESIDENCES

38. Based on a review of information obtained from Instagram (Facebook) and other electronic service providers, **TARGET SUBJECTS** Yusef **GALES-BEY**, Dequan **ELLIS**, and Darrelle **RICH,** as well as another person, Daquan **YOUNG** (a juvenile) were identified as being associated with one or more email accounts and/or telephone numbers linked to Instagram pages that posted/facilitated the posting of extortion demands/threats or identified/facilitated the identification of victims and witnesses to crimes using derogatory terms such as snitch or rat.

*Yusef **GALES-BEY***

39. As detailed above, Instagram account "ratsofbmoe1" made several public posts demanding Cash App payments in exchange for not posting victim information. On September 3, 2020 at 10:39am, "ratsofbmoe1" posted, "I'm doin deal before 12 pm 75$ I take ya paper work down for a day <*laughing emoji, laughing emoji, male facepalm emoji*> stack I delete it for good

[3] Confidential Source 1 (CS-1): CS-1 began cooperating with the FBI in 2019 and previously cooperated with a state law enforcement agency. CS-1 is associated with multiple members of a drug conspiracy/organization located in Baltimore, Maryland. The information provided by CS-1 has been found to be reliable and has been corroborated by other investigative means. CS-1 receives financial compensation in return for cooperation on drug-related matters, however because CS-1 is a victim in this case, CS-1 has not been financially compensated for any assistance provided related to the extortion investigation. CS-1 has numerous convictions for crimes of violence, theft, and other drug-related crimes.

stomp y'all fkn feet." According to records provided by Facebook, the post was uploaded using Comcast IP address 73.135.195.194. Further, a review of IP logins for "ratsofbmoe1" on September 3, 2020 identified Comcast IP address 2603:3003:1cb8:6000:b8f2:2b5b:52c5:5704 used to log into the account at approximately 2:34pm. On February 16, 2021, Comcast provided subscriber information for the two IP addresses at the precise times that they were used to upload information to or log into "ratsofbmoe1." Comcast IP address 73.135.195.194 was subscribed to Catherine Ware at address 602 W. Franklin Street, Apartment 5, Baltimore, Maryland 21201 and telephone number 443-882-0825. Comcast IP address 2603:3003:1cb8:6000:b8f2:2b5b:52c5:5704 was subscribed to "Bey Brothers Mortgage Com" at address 6305 Belair Rd. Ste. 3, Baltimore, Maryland 21206 and associated telephone number 410-258-1259 (**SUBJECT TELEPHONE 1**).

40. Subscriber information for "ratsofbmoe1" provided by Facebook listed beybrothers410@gmail.com as the email address associated with the account. Subscriber information for beybrothers410@gmail.com provided by Google indicated the account was created on August 1, 2017, with account name "Yungk410bey" and birthday February 9, 1988. Additional Instagram accounts identified as linked to beybrothers410@gmail.com included "ratsofbmoe", "ratsofbmore", and "darealratsofbmore." Additional Instagram accounts linked to **SUBJECT TELEPHONE 1** included "ratsofbmore" and "ratsofbmore1."

41. A review of messages sent by Instagram account "r.s.n_yungk", which was associated with email address getdownmusicgroup410@gmail.com, revealed messages on December 19, 2020, where the account user stated, "I grab one u come out", followed by, "2700 Mura st." On December 22, 2020, Apple provided subscriber records associated with

getdownmusicgroup410@gmail.com, which listed **SUBJECT TELEPHONE 1** as the telephone number associated with the account.

42. An open source query of Maryland business registrations revealed "Yusef Gales Bey" registered "Bey Brothers Mortgage, LLC" on December 16, 2019 with address 6210 Robin Hill Rd., Baltimore, Maryland and business address 541 E. Patapsco Ave. Suite 201, Baltimore, Maryland. An inquiry with the Maryland Department of Public Safety and Correctional Services revealed Yusef **GALES-BEY** was under the supervision of a probation officer as recently as March 2019 for a drug conviction in 2015. On February 14, 2019, **GALES-BEY** reported his telephone number as **SUBJECT TELEPHONE 1** and his address was 6210 Robin Hill Rd. Baltimore, Maryland to law enforcement as part of an unrelated matter. **GALES-BEY's** date of birth matches the date of birth provided by the registered user of beybrothers410@gmail.com.

43. On November 28, 2020, Yusef **GALES-BEY** filed a complaint with the Westminster Police Department related to a child custody issue. At time of the report, GALES-BEY provided his telephone number as 410-627-4860 and his address as 2700 Mura Street, Baltimore, Maryland (**TARGET RESIDENCE 1**).

44. On April 14, 2021, PayPal provided subscriber records associated with **SUBJECT TELEPHONE 1**, which included PayPal account number 1164470257234928168, with subscriber email address beybrothersmortgage@gmail.com, and user "Yusef Gales Bey" with home address 6210 Robin Hill Road, Baltimore, Maryland and a gift address of **TARGET RESIDENCE 1**. The PayPal account was created and the gift address was entered on October 28, 2020. **SUBJECT TELEPHONE 1** was listed as "Confirmed."

45. On January 12, 2021, Cash App provided subscriber information for a Cash App account associated with **SUBJECT TELEPHONE 1**. Cashtag "allthere443" was associated with

subscriber name "Yusef Gales Bey"; date of birth February 9, 1988; and address 6210 Robin Hill Road, Baltimore, Maryland. A review of Cash App transactions sent to and from the account did not reveal any money transfers that contained memo information indicating they were extortion payments. However, multiple payments were received from Cash App user "Catherine Ware" (subscriber of the IP address used to upload the extortionate post mentioned in paragraph 35 on September 3, 2020).

46. On February 4, 2021, Sprint provided subscriber information and toll records for **SUBJECT TELEPHONE 1**, which indicated the phone number was active and subscribed to "Donte Brown", subscriber address 1117 Tiffany Ct. Baltimore, Maryland 21201. The device was listed as having IMEI 354917095178240, which resolves to an Apple iPhone 7, Model A1660 (**SUBJECT DEVICE 1**). According to call records provided by Sprint, one of the top five callers for **SUBJECT TELEPHONE 1** is 443-882-0825 (the telephone number provided by Catherine Ware, subscriber of the IP address used to upload the extortionate post mentioned above on September 3, 2020). A review of individuals associated with 1117 Tiffany Ct. Baltimore, Maryland conducted using law enforcement databases indicated possible resident "Donte Brown" with date of birth February 9, 1988 (the same date of birth as provided for Cash App and Google accounts linked to **GALES-BEY**). A review of Maryland Motor Vehicle Administration records failed to locate an individual with the name "Donte Brown" and date of birth February 9, 1988. Further review of Maryland Motor Vehicle Administration records determined Yusef Ali **GALES-BEY** has a valid Maryland Driver's License with listed date of birth February 9, 1988 and address 6210 Robin Hill Rd. Gwynn Oak, Maryland.

47. Physical surveillance was conducted at 6210 Robin Hill Road, Baltimore, Maryland on March 24, 2021. A blue Honda bearing Maryland registration 4DN9655 was observed parked

on the property in a covered spot. According to Maryland Motor Vehicle Administration (MVA) checks, the registered owner of the vehicle was determined to be Yvonne Gales-Bey, with address 6210 Robin Hill Road, Baltimore, Maryland. Law enforcement database checks list Yvonne Gales-Bey as the possible mother of Yusef **GALES-BEY**.

48. On March 22, 2021, United States Magistrate Judge Hon. A. David Copperthite of the District Court of Maryland authorized search warrants for GPS ping data and the use of a cell site simulator for **SUBJECT TELEPHONE 1** (associated with **GALES-BEY**), **SUBJECT TELEPHONE 2** (associated with **ELLIS**), **SUBJECT TELEPHONE 3** (associated with **RICH**), and another phone number associated with Daquan **YOUNG**. Location data for **SUBJECT TELEPHONE 1** was obtained from Sprint beginning on March 24, 2021. Since that time, an analysis of GPS "ping" data (carrier provided location-based services, described further below) for approximately three weeks has determined **SUBJECT TELEPHONE 1** is most frequently located near the intersection of N. Lakewood Avenue and E. Preston Street in Baltimore, with a consistent radius of 72 meters (approximately .0441 miles or 236 feet). During that time, **SUBJECT TELEPHONE 1** has consistently been located in this area with the above radius during the overnight hours of midnight until 6:00am. The center of the radius is approximately 400 feet from **TARGET RESIDENCE 1**, and the outer portion of the radius terminates at the alley behind **TARGET RESIDENCE 1**, placing **TARGET RESIDENCE 1** just outside the radius.

49. Physical surveillance was conducted at **TARGET RESIDENCE 1** on April 9, 2021. A Honda Accord bearing Maryland registration 2EA9678 and an Acura MDX bearing Maryland registration 9EH2498 were observed parked on the property. According to MVA checks, the registered owner of the 2006 Honda Accord is Yusef Ali **GALES-BEY** at 6210 Robin

Hill Road, Gwynn Oak, Maryland, 21207, and the registered owner of the 2004 Acura MDX is Bey Brothers Mortgage LLC, at 6305 BelAir Road, Baltimore, Maryland 21206.

50. A spot check was conducted at **TARGET RESIDENCE 1** on April 14, 2021 at approximately 4:55pm. A red Nissan Sentra bearing Maryland registration 4EL7336 and an Acura MDX bearing Maryland registration 9EH2498 were observed parked on the property. Physical surveillance was conducted at the location at approximately 5:30pm. A black male matching the description of Yusef **GALES-BEY** was observed near the rear door of the residence, and then entered a red Nissan Sentra parked on the property and drove away. (According to MVA checks, the registered owner of the Nissan Sentra is Ikeda Benjamin at 848 Abbott Court, Baltimore, Maryland.) Shortly after this person was observed, investigators checked the GPS "ping" data which showed that **SUBJECT TELEPHONE 1** was located near the intersection of N. Lakewood Avenue and E. Preston Street in Baltimore with a radius of approximately 71 meters at 5:22pm. The next "ping" registered from **SUBJECT TELEPHONE 1** located it across town in East Baltimore at 6:07pm, with a radius of approximately 443 meters. This is consistent with the observation of the person matching **GALES-BEY's** description having driven away in the Nissan Sentra. The subscriber address for **SUBJECT TELEPHONE 1**, 1117 Tiffany Ct. Baltimore, Maryland, is located within this radius.

51. A spot check was conducted at **TARGET RESIDENCE 1** on April 16, 2021 at approximately 4:50am. An Acura MDX bearing Maryland registration 9EH2498 was observed parked on the property. An analysis of GPS "ping" data determined **SUBJECT TELEPHONE 1** was located near the intersection of N. Calvert Street and E. Eager Street in the Mount Vernon area of Baltimore at 5:07am, with a radius of approximately 201 meters. The next "ping" registered from **SUBJECT TELEPHONE 1** was located near the intersection of N. Lakewood

Avenue and E. Preston Street in Baltimore with a radius of approximately 71 meters at 5:37am. A second spot check was conducted at **TARGET RESIDENCE 1** at 6:00am. A red Nissan Sentra bearing Maryland registration 4EL7336 and an Acura MDX bearing Maryland registration 9EH2498 were observed parked on the property.

52. An inquiry for the utilities subscriber at **TARGET RESIDENCE 1** on April 15, 2021, returned results for "Yuses A. Gales-Bey."[4]

*Dequan **ELLIS***

53. As detailed above, Instagram account "ratsofbmoe3" communicated with "ratsofbmoe1" about "backing up" information and sharing a password, suggesting the accounts were controlled by two different individuals working together. According to records provided by Facebook, "ratsofbmoe3" and "returnoftherats_ofbmoe" listed dequanellis40@icloud.com and 443-469-0171 (**SUBJECT TELEPHONE 2)** as the email address and telephone number associated with the accounts.

54. On December 15, 2020, in response to a federal search warrant, Apple provided account information for Apple ID dequanellis40@icloud.com, which listed **SUBJECT TELEPHONE 2** as the telephone number associated with the account. Apple also provided the IMEI for the cellular device associated with the account as 356137097451595.

55. On February 4, 2020, Sprint provided subscriber information for **SUBJECT TELEPHONE 2**, which indicated the phone number was active and subscribed to Dequan **ELLIS**, subscriber address 2777 The Alameda, Baltimore, Maryland 21218. The device was listed as

[4] "Yuses" is so spelled in the records. I note that "Yuses" is one letter off from "Yusef" and that the "s" key on a standard keyboard is in the same row as the "f" key, and those two letters are separated by one key, "d".

having an Electronic Serial Number of 089556352907623001, which resolves to an IMEI of 356137097451595 (the same as provided by Apple on December 15, 2020 pursuant to a search warrant for dequanellis40@icloud.com) for an Apple iPhone 6S, Model A1688 (**SUBJECT DEVICE 2**). According to law enforcement databases, Dequan **ELLIS** was associated with that address from 2009-2015. A review of Maryland Motor Vehicle Administration records determined Dequan Michael **ELLIS** has a valid Maryland State ID at address 739 N Kenwood Ave, Baltimore, Maryland 21205 (**TARGET RESIDENCE 2**).

56. Pursuant to the federal search warrant for a pen register and location data for **SUBJECT TELEPHONE 2**, Sprint provided data beginning on March 24, 2021. Since that time, an analysis of GPS "ping" data for approximately three weeks has determined **SUBJECT TELEPHONE 2** is most frequently located in East Baltimore, within a radius of 3,067 meters, or 1.89 miles. Specifically, **SUBJECT TELEPHONE 2** has registered this consistent radius each day, centered near the intersection of E. Eager Street and N. Linwood Avenue in Baltimore during the hours of midnight until 6:00am. **TARGET RESIDENCE 2** is within this radius.

57. Physical surveillance was conducted at **TARGET RESIDENCE 2** from approximately 6:00am to 6:30am on April 12, 2021 to April 16, 2021. Each morning, an individual was observed exiting the residence and getting into a different vehicle. At least one vehicle displayed a placard or sign indicating it was a rideshare (e.g. Uber or Lyft). On April 15, 2021, the occupant of **TARGET RESIDENCE 2** was dropped off near the University of Maryland, Baltimore Police Department, located at 214 N. Pine Street, Baltimore, Maryland. On April 15, 2021, a representative from the University of Maryland, Baltimore Police Department confirmed Dayshawn Ellis was employed there as an unarmed security guard.

58. A review of records from the Maryland Department of Public Safety and Correctional Services (DPSCS) revealed the mother of Dequan **ELLIS** was identified as Cynthia Fulton. A review of open source information identified Elma McDonald as the likely mother of Cynthia Fulton (i.e. the maternal grandmother of **ELLIS**). A review of records from the Maryland Department of Assessments and Taxation determined **TARGET RESIDENCE 2** was owned by Elma Ruth Fulton McDonald. Dayshawn Ellis, believed to reside at **TARGET RESIDENCE 2** based on physical surveillance, shares the same birthday with Dequan **ELLIS**, and has a social security number one digit lower than **ELLIS**, indicating she is likely his twin sister.

59. Physical surveillance was conducted at **TARGET RESIDENCE 2** on April 14, 2021. At approximately 5:18pm, a black male matching the description of Daquan **ELLIS** was observed existing **TARGET RESIDENCE 2**, crossing Kenwood Avenue, and walking southbound on Kenwood Avenue. An analysis of "ping" data on April 14, 2021 at 5:18pm located **SUBJECT TELEPHONE 2** near the intersection of E. Eager Street and Linwood Avenue, with a radius of 3,035 meters. **SUBJECT RESIDENCE 2** is within this radius.

*Darelle **RICH***

60. As detailed above, on September 30, 2020 Instagram account "ratsofbmoe4" posted a victim photograph followed by the threat, "kill all rats." According to records provided by Facebook, "ratsofbmoe4", "410rats", "ratsofbmoe410", "wzone_legend", "wzonetrapper", and "travonjones" listed 443-897-8389 (**SUBJECT TELEPHONE 3**) as the telephone number associated with the accounts. Instagram account "travonjones" was registered with email address darnellrichardson7@gmail.com.

61. According to records provided by Facebook, a review of IP logins for "ratsofbmoe4" on October 1, 2020 identified Comcast IP address

2601:14d:4103:71a0:edb7:5a8d:b195:dd65 used to log into the account at approximately 9:04pm. On February 16, 2021, Comcast provided subscriber information for that IP address, which was subscribed to Tadesha Brinkley at address 5116 Pembridge Avenue, Baltimore, MD 20215 (**TARGET RESIDENCE 3**) and telephone number 443-414-6668. A review of other Instagram posts by "ratsofbmoe4" on September 12, 2020 and September 16, 2020 returned similar results from Comcast, indicating the IP addresses were dynamically assigned, but also subscribed to Tadesha Brinkley at **TARGET RESIDENCE 3**.

62. On January 12, 2021, Cash App provided subscriber information for Cashtag "darrellerich", which was associated with subscriber name "Darrelle Christopher Rich"; date of birth January 28, 1990; address as **TARGET RESIDENCE 3**; and telephone number as **SUBJECT TELEPHONE 3**.

63. An inquiry with the Maryland Department of Public Safety and Correctional Services revealed **RICH** was under the supervision of a probation officer as recently as May 2020 for a local drug conviction in 2019. On May 14, 2020, **RICH** reported his telephone number as **SUBJECT TELEPHONE 3**.

64. On December 4, 2020, in response to a subpoena, Sprint provided subscriber information for **SUBJECT TELEPHONE 3**, which indicated the phone number was subscribed to "Travon James", subscriber address as **TARGET RESIDENCE 3**, with service cancelled on June 19, 2020. On January 26, 2021, in response to a subpoena, AT&T provided subscriber information for **SUBJECT TELEPHONE 3**, which indicated a service start date of June 19, 2020 to subscriber "Tracfone Wireless" at address 8390 NW 25th St. Miami, Florida 33122. Open source research returned results associating that address as a business address for Tracfone Wireless. AT&T records listed the device associated with **SUBJECT TELEPHONE 3** as having

an IMEI of 353815083965804, which resolves to an Apple iPhone 7Plus, Model A1784 (**SUBJECT DEVICE 3**).

65. According to call records provided by AT&T, one of the top callers for **SUBJECT TELEPHONE 3** is 443-414-6668 (the telephone number provided by Tadesha Brinkley, subscriber of the IP address mentioned in paragraph 45 on October 1, 2020). Open search queries for "Darrelle Rich" returned results at www.registry.thebump.com for "Tadesa Brinkley & Darrelle Rich's Baby Registry" at Target, with due date October 7, 2020 and location Baltimore, Maryland.

66. A review of Maryland Motor Vehicle Administration records determined Darrelle Christopher **RICH** has a valid Maryland Learner's Permit with listed date of birth January 28, 1990 and address as **TARGET RESIDENCE 3**.

67. On March 31, 20201, a trash cover was conducted at **TARGET RESIDENCE 3**. Items observed in the trash included mail addressed to Darrelle **RICH** and Tadesa Brinkley.

68. Pursuant to the federal search warrant for a pen register and location data for **SUBJECT TELEPHONE 3**, AT&T provided data beginning on March 30, 2021. Since that time, an analysis of GPS "ping" data for approximately two weeks has determined **SUBJECT TELEPHONE 3** is most frequently located in the area around the Pimlico Race Course in the Park Heights Area of Baltimore, with a radius ranging from 88 meters, or .05 miles to approximately 492 meters, or .30 miles. During this time, **SUBJECT TELEPHONE 3** has consistently been located within this radius range during the hours of midnight until 6:00am. **TARGET RESIDENCE 3** is within the smaller radius range of 88 meters.

Status of Instagram Pages

69. As of March 2021, the majority of the above Instagram pages have been removed or shut down by Instagram in response to complaints filed by other Instagram users, as well as law enforcement requests. Preservation requests were previously filed for all pages, therefore it is anticipated subscriber information and page content will still be available in response to federal legal process.

70. Based on a review of Instagram and social media account activity to date, I believe the **TARGET SUBJECTS** intended to expose the identities of cooperators and/or extort money from potential victims posted online as well as other victims not yet posted or identified. The Instagram posts also contain threats designed to injure the reputation of the victims, to include deceased persons, and in at least one case issued a death threat to a victim. It is still unknown how many victims were featured on private pages, how many victims have been directly contacted or threatened by the Instagram user(s) of those pages, or how many victims have provided payment in order to remove their information or prevent their information from being posted.

71. Based on the information provided above, I believe the **TARGET SUBJECTS** are involved in creating, advertising, maintaining, and facilitating public and private extortionate posts on Instagram targeting individuals alleged to be federal and state law enforcement cooperators. In my experience, subjects who commit extortion tend to keep and store communications and other information in their residences and on their phones well after the completion of such crimes and continue to communicate through their phones or other means about their crimes after the crimes have been completed. Thus, I believe that there is information contained in the **TARGET RESIDENCES** and on the **SUBJECT TELEPHONES** that may still contain evidence relevant to the investigation of the **TARGET OFFENSES**.

CELL PHONES, ELECTRONIC STORAGE, FORENSIC ANALYSIS, AND BIOMETRIC UNLOCKING

72. As discussed earlier in this affidavit, investigators have identified various cellular phones used by the **TARGET SUBJECTS**. The following chart summarizes the **SUBJECT TELEPHONES** and **SUBJECT DEVICES** used by the **TARGET SUBJECTS**, as discussed previously in this affidavit:

TARGET SUBJECT/USER	SUBJECT TELEPHONE	SUBJECT DEVICE
Yusef GALES-BEY	410-258-1259	IMEI 354917095178240
Dequan ELLIS	443-469-0171	IMEI 356137097451595
Darrelle RICH	443-897-8389	IMEI 353815083965804

73. I believe the above-described phones constitute evidence of the **SUBJECT OFFENSES** because possession of the phones will evidence the identity of the users of the phones. Recovering and examining these phones is critical to uncovering further evidence and will also establish a particular phone user's role in the commission of the **SUBJECT OFFENSES**.

74. Investigators believe that while the above-described phones will contain fruits and evidence of the **SUBJECT OFFENSES**, it is also likely that other cellular telephones currently utilized by the **TARGET SUBJECTS** likely contain similar evidence of the **SUBJECT OFFENSES**. I also believe that other devices used by the **TARGET SUBJECTS** will contain evidence of the **SUBJECT OFFENSES** because, as noted above, phones often import data from prior phones (i.e. contact lists, photos, messages, applications, etc.). Therefore, this warrant authorizes the search and seizure of: (a) the **SUBJECT DEVICES**; (b) any cell phones, computers, and storage media found in the bedroom or sleeping quarters of the **TARGET SUBJECTS** within their respective **TARGET RESIDENCES**; (c) any cell phones, computers,

and storage media found on the persons of the **TARGET SUBJECTS**; (d) any cell phones, computers, and storage media found in close proximity to the **TARGET SUBJECTS**, or in close proximity to a space the **TARGET SUBJECTS** had recently occupied; (e) any cell phones, computers, and storage media found in the **TARGET RESIDENCES** that through circumstances and investigation is reasonably believed to be/have been owned, used or accessed by the **TARGET SUBJECTS** ;and (f) any cell phones, computers, and storage media identified by the **TARGET SUBJECTS**, or another occupant/resident of the **TARGET RESIDENCES** as belonging to the **TARGET SUBJECTS** (collectively the **"DEVICES**").

75. As described above and in **Attachment B**, this application seeks authorization to search for contraband, evidence, fruits, and instrumentalities of the **SUBJECT OFFENSES** that might be found on the **DEVICES** in whatever form they are found. One form in which the evidence might be found is as records in the form of data stored on a cell phone, a computer's hard drive, or other storage media. Thus, the warrant applied for would authorize the seizure and search of cell phones, computers, and storage media and, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

76. Probable cause. I submit that if a cell phone, computer, or storage medium is found in the **TARGET RESIDENCES** and/or the persons of the **TARGET SUBJECTS**, there is probable cause to believe those records will be stored on that cell phone, computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.

Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

77. *Forensic evidence.* As further described in **Attachment B**, this application seeks permission to locate not only cell phone and computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the cell phones and computers were used, the purpose of their use, who used them, and when.

There is probable cause to believe that this forensic electronic evidence will be on the **DEVICES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a cell phone, computer, and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or

storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations; computer activity associated with user accounts; electronic storage media that connected with the computer; and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of

mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a cell phone or computer works can, after examining this forensic evidence in its proper context, draw conclusions about how cell phones or computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a cell phone or computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or

absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

78. Necessity of seizing or copying entire computers or storage media. In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

79. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, and/or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Biometric Unlocking

80. I am further seeking permission, pursuant to these warrants to permit law enforcement to, using a device's biometric features, compel the **TARGET SUBJECTS** to unlock: (a) any of the **DEVICES**. I seek this authority based on the following:

81. From training and experience, I also know that users of cellular devices also carry their cell phones on their persons or keep them in close proximity so they can access them.

82. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

83. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch.

84. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face.

Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

85. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

86. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

87. As discussed in this affidavit, I have reason to believe that the above-described **DEVICES** are in the possession of the **TARGET SUBJECTS** and that they will be found during the search of the **TARGET RESIDENCES** or the searches of the **TARGET SUBJECTS**' persons. The passcodes or passwords that would unlock the cell phones subject to search under this warrant currently are not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the cell phones, making the use of biometric features necessary to the execution of the search authorized by this warrant.

88. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel discover that a **DEVICE** is locked and is equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

89. Based on the foregoing, if law enforcement personnel encounter the cell phones described above pursuant to this warrant and the phones may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to obtain from the **TARGET SUBJECTS**, the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock the **DEVICES**, including to (1) press or swipe the fingers (including thumbs) of the aforementioned person(s) to the fingerprint scanner of the **DEVICES**; (2) hold the **DEVICES** in front of the face of the **TARGET SUBJECTS** to activate the facial recognition feature; and/or (3) hold the **DEVICES** in front of the face of the **TARGET SUBJECTS** to activate the iris recognition feature, for the purpose of attempting to unlock the **DEVICES** in order to search the contents as authorized by this warrant.

90. The proposed warrant does not authorize law enforcement to require that the **TARGET SUBJECTS** state or otherwise provide the password or identify specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the **DEVICES**. Nor does the proposed warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) would be permitted under the proposed warrant. To avoid confusion on that point, if agents in executing the warrant ask the **TARGET SUBJECTS** for the passwords to the cell phones, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks the cell phones, the agents will not state or otherwise imply that the warrant requires the person to provide such information and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

AUTHORIZATION REQUEST

91. I submit that there is probable cause to believe that violations of the **SUBJECT OFFENSES** have been committed by the **TARGET SUBJECTS** and that there is probable cause to search the persons of the **TARGET SUBJECTS** and the **TARGET RESIDENCES** as further described in **Attachment B**. I further submit that there is probable cause to believe that evidence, fruits, and instrumentalities of these crimes will be found in the **DEVICES.**

Special Agent Summer Baugh
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 19 day of April, 2021.

Honorable Thomas M. DiGirolamo
United States Magistrate Judge

ATTACHMENT A-1

Location to be Searched: TARGET RESIDENCE 1

TARGET RESIDENCE 1 is located at **2700 Mura Street, Baltimore, Maryland 21213**. The property consists of a two-story brick rowhome end unit with white awnings and steps leading to a front door that has a black wrought iron security door.

ATTACHMENT A-2

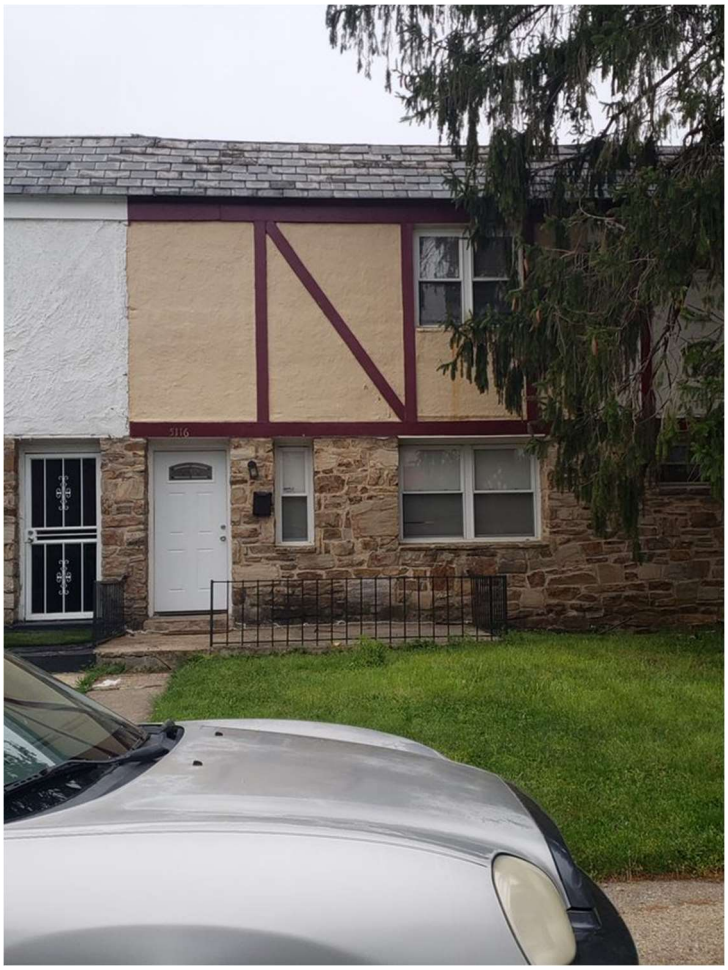
Location to be Searched: TARGET RESIDENCE 2

TARGET RESIDENCE 2 is located at **739 N. Kenwood Avenue, Baltimore, Maryland 21205**. The property consists of a two-story brick rowhome with white awnings and steps leading to a front door with a white wrought iron security door.

ATTACHMENT A-3

Location to be Searched: TARGET RESIDENCE 3

TARGET RESIDENCE 3 is located at **5116 Pembridge Avenue, Baltimore, Maryland 21215**. The property consists of a two-story stone and tan color rowhome with one step leading to a white front door.



ATTACHMENT A-4

Person to be Searched

Yusef GALES-BEY, a man born February 9, 1988 and assigned an FBI number ending in 3FC8.

ATTACHMENT A-5

Person to be Searched

Dequan ELLIS, a man born June 24, 1991 and assigned an FBI number ending in 6PD7.

ATTACHMENT A-6

Person to be Searched

Darrelle RICH, a man born January 28, 1990 and assigned an FBI number ending in 6PC3.

ATTACHMENT B

ITEMS AND INFORMATION TO BE SEIZED AND SEARCHED

All items and information found in **TARGET RESIDENCE 1 (described in Attachment A-1), TARGET RESIDENCE 2 (described in Attachment A-2), TARGET RESIDENCE 3 (described in Attachment A-3), (**collectively, "the **TARGET RESIDENCES**"), and the persons of **Yusef GALES-BEY (described in Attachment A-4), Dequan ELLIS (described in Attachment A-5), Darrelle RICH, and (described in Attachment A-6**) that are or contain evidence of a crime, fruits of a crime, or instrumentalities of the crimes of Interstate Threats (18 U.S.C. § 875); Obstruction of Justice (18 U.S.C. § 1503); and Witness Tampering (18 U.S.C. §§ 1512, 1513) (collectively, "the **SUBJECT OFFENSES**"), including the following:

1. Records relating to the violations described above, including:
    a. Documents, records, or information relating to an extortion demand or payment;
    b. Documents, records, or information relating to the acquisition, possession, or distribution of court paperwork;
    c. Mailings, communications, letters, and correspondence sent or received to or by persons detained or incarcerated in correctional and detention facilities *or* send or received by persons who are employed by correctional and detention facilities;
    d. Documents, records, or information relating to communications with co-conspirators, including wire, electronic, and written communications;
    e. Documents, records, or information relating to identities of victims and/or co-conspirators, including photographs, contact information, addresses, calendars, and identification documents;
    f. Financial records, including bank records, checks, credit card bills, account information, safe deposit boxes, and any other items reflecting the obtaining, secreting, transfer, and/or concealment of assets;
    g. Documents, items, records, or information relating to indicia of occupancy, residency, and ownership or use of the **TARGET RESIDENCES**, including, but not limited to, utility and telephone bills, cancelled envelopes, rental, purchase, or lease agreements, identification documents, and keys; and
    h. Documents, records, or information that are evidence of ownership or use of digital devices found in the **TARGET RESIDENCES**;
    i. Documents, items, records, or information related to pending or closed court cases, including but not limited to cooperation with law enforcement, the identity of witnesses.

j. Documents, items, records, or information related to the use or ownership of electronic accounts, such as Instagram accounts

2. Safes or other locked storage containers that may contain any of the items referenced herein, as well as keys or other items used to access these locations, including keys to any vehicles to be searched pursuant to the warrant.

3. All cell phones, computers, and storage media (as defined below) identified as belonging to Yusef **GALES-BEY** (described in **Attachment A-4**), Dequan **ELLIS** (described in **Attachment A-5**), and Darrelle **RICH** (described in **Attachment A-6**), including the following:
   a. Any cell phones, computers, and storage media found on the persons of **GALES-BEY**, **ELLIS**, **or RICH**;
   b. Any cell phones, computers, and storage media found in the bedroom or sleeping quarters of **GALES-BEY**, **ELLIS**, or **RICH**;
   c. Any cell phones, computers, and storage media found in close proximity to **GALES-BEY**, **ELLIS**, **or RICH**, or in close proximity to a space that **GALES-BEY, ELLIS,** or **RICH** had recently occupied;
   d. any cell phones, computers, and storage media found in the **TARGET RESIDENCES** that through circumstances and investigation is reasonably believed to be/have been owned, used or accessed by the **GALES-BEY, ELLIS, or RICH**;
   e. Any cell phones, computers, and storage media identified by **GALES-BEY**, **ELLIS**, or **RICH** or another occupant/resident of the **TARGET RESIDENCES** as belonging to **GALES-BEY**, **ELLIS**, or **RICH**;
   f. The cellular telephone assigned call number 410-258-1259, and/or IMEI 354917095178240, (hereinafter, "**SUBJECT DEVICE 1**");
   g. The cellular telephone assigned call number 443-469-0171, and/or IMEI 356137097451595 (hereinafter, "**SUBJECT DEVICE 2**");
   h. The cellular telephone assigned call number 443-897-8389, and/or IMEI 353815083965804 (hereinafter, "**SUBJECT DEVICE 3**");
   i. any and all adapters, chargers, or other hardware items necessary to charge the battery, or to maintain the functioning of the **DEVICES**;

The above-described cell phones, computers, and storage media are referred to herein as the "DEVICES." The warrant also authorizes the search of the **DEVICES** for the following:

a. evidence of who used, owned, or controlled the **DEVICES** at the time the things described in this warrant were created, edited, or deleted, such as

logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. Call logs reflecting date and time of received calls;

c. Any and all digital images and videos of persons associated with this investigation;

d. Text messages to and from the **DEVICES** that refer or relate to the crimes under investigation;

e. Records of incoming and outgoing voice communications that refer or relate to the crimes under investigation;

f. Voicemails that refer or relate to the crimes under investigation;

g. Voice recordings that refer or relate to the crimes under investigation;

h. Any data reflecting the **DEVICES'** locations;

i. Contact lists;

j. Any and all records related to the location of the user(s) of the devices;

k. evidence of software that would allow others to control the **DEVICES**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

l. evidence of the lack of such malicious software;

m. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

n. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

o. evidence of the attachment to the **DEVICES** of other storage devices or similar containers for electronic evidence;

p. evidence of programs (and associated data) that are designed to eliminate data from the **DEVICES**;

q. evidence of the times the **DEVICES** were used;

r. passwords, encryption keys, and other access devices that may be necessary to access the **DEVICES** that are found stored within the **DEVICES**

s. records of or information about Internet Protocol addresses used by the **DEVICES**;

t. records of or information about the **DEVICES'** Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

u. contextual information necessary to understand the evidence described in this attachment;

v. records and information relating to the **SUBJECT OFFENSES**;

w. records and information relating to the identity or location of the persons suspected of violating the statutes described above;

x. records and information related to the use or ownership of social media and electronic accounts, such as Instagram, Cash App, etc.

y. Records, information, and items relating to violations of the statutes described above including data from third-party applications (including social media applications like Facebook and Instagram and messaging programs like WhatsApp and Snapchat).

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

DEVICE UNLOCK: During the execution of the search of the **TARGET RESIDENCES** and persons of **Yusef GALES-BEY (described in Attachment A-4), Dequan ELLIS (described in Attachment A-5), Darrelle RICH (described in Attachment A-6)**, and with respect to any of the **DEVICES** described in this attachment, law enforcement personnel are authorized to search the **DEVICES** and unlock them by: (1) pressing or swiping the fingers (including thumbs) of **GALES-BEY**, **ELLIS**, **and/or RICH** to the fingerprint scanner of the **DEVICES**; (2) holding the **DEVICES** in front of the face of **GALES-BEY**, **ELLIS**, **and/or RICH** to activate the facial recognition feature; and/or (3) holding the **DEVICES** in front of the face of **GALES-BEY**, **ELLIS**, **and/or RICH** to activate the iris recognition feature, for the purpose of attempting to unlock the device(s), and attempting to access data contained in the **DEVICES**, in order to search the contents as authorized by these warrants.

With respect to the search of any of the cell phones, computers and items described above (including the **DEVICES**) which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the

following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, to minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. Surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
c. "scanning" storage areas to discover and possible recover recently deleted files;
d. "scanning" storage areas for deliberately hidden files; or
e. Performing keyword searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the **SUBJECT OFFENSES** other criminal activity, or evidence of who owns or uses the device, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

Items of potential forensic value will be recovered and processed using a variety of means employed by forensic evidence technicians and specialists. Recovery of these items may result in damage to property. These recovery methods may include, but are not limited to, removing sections of tile, flooring, drywall, plaster, drain plumbing, or by employing other methods of recovery in locations where investigators believe the presence of forensic evidence may be present.